Published and Copyright (c) 1999 - 2013
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1521 05/31/13

~ Cyber Threats Danger! ~ People Are Talking! ~ New Google Probe!
~ Ireland Rejects Claims! ~ USSR's Old Domain Name ~ Win 8.1 Features!
~ Linked In Passwod Train! ~ Hate Speech Crackdown! ~ Social Media Bill!

~ Sick of Password Typing? ~ Wearable Technology? ~ New Gmail Inbox!

-* 'Atari Dump' To Be Excavated! *-
-* Maine Teens Wary of Social Media Now *-
-* Pentagon Programs Target of Cyber Threat! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Memorial Day weekend has passed, marking the unofficial beginning of summer. So, what could happen to "validate" this? How about a heat wave? Yep, the forecast is for temperatures in the 90's over the next few days. If today was any indication of what we'll be facing, we're in for some hot weather! We hit at least 95 degrees here in northeast Massachusetts today; the AC is running at full blast to take a bite out of this heat!

So, while I try to find a way to keep cool while putting this week's issue to bed, you can sit back and relax, hopefully!

Until next time...

=~=~=~=

->In This Week's Gaming Section
"""""""""""""""""""""""""""""""

- Publishers To Receive Cut of Xbox One Pre-owned Sales!
- Developers Address Video Game Violence in New Film!
- 'Atari Dump' Will Be Excavated, After Nearly 30 Years!
- And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

Publishers To Receive Cut of Xbox One Pre-owned Sales at Retail

Retailers will be free to charge whatever they wish for pre-owned Xbox One games, but both Microsoft and publishers will take a percentage cut of every sale.

Retail sources have told MCV that Microsoft has this week briefed key retail partners on how it intends to take ownership of the pre-owned market.

This is how we ve been told it will all work:

A gamer walks into a retailer and hands over the game they wish to sell. This will only be possible at retailers who have agreed to Microsoft s T&Cs and more importantly integrated Microsoft s cloud-based Azure pre-owned system into its own.

The game is then registered as having been traded-in on Microsoft s system. The consumer who handed it over will subsequently see the game wiped from their account hence the until now ambiguous claim from Phil Harrison that the Xbox One would have to check in to Microsoft s servers every 24 hours.

The retailer can then sell the pre-owned game at whatever price they like, although as part of the system the publisher of the title in question will automatically receive a percentage cut of the sale. As will Microsoft. The retailer will pocket the rest.

Unconfirmed reports on ConsoleDeals.co.uk suggest that retail s slice will be as little as ten per cent. That s a significant cut from what it has become accustomed to from pre-owned sales and more in line with what they would receive from the sale of a new game hence, the value of the pre-owned market to the retailer is effectively destroyed.

These same unconfirmed reports also suggest that the activation cost for consumers buying or borrowing pre-owned software will be £35.

When contacted by MCV Microsoft responded with the following statement:
 We know there is some confusion around used games on Xbox One and wanted to provide a bit of clarification on exactly what we ve confirmed.

"While there have been many potential scenarios discussed, we have only confirmed that we designed Xbox One to enable our customers to trade in and resell games at retail. Beyond that, we have not confirmed any specific scenarios. Another piece of clarification around playing games at a friend s house should you choose to play your game at your friend s house, there is no fee to play that game while you are signed in to your profile.

Many readers are asking whether the £35 will be additional cost on top of the price of buying the game. No, we believe that the £35 figure which is not our number, incidentally would cover the entire transaction. If correct this would leave retail with a cut per sale of around £3.50.

Microsoft’s Major Nelson has at last offered a direct (although not direct to MCV, incidentally) reply to our story on his website. It reads:

 Over the past few days, we have been reading comments and message boards following the Xbox One announcement. There are a few questions regarding used games. I wanted to clarify and provide this official statement:

 The ability to trade in and resell games is important to gamers and to Xbox. Xbox One is designed to support the trade in and resale of games. Reports about our policies for trade in and resale are inaccurate and incomplete. We will disclose more information in the near future.

Is this a dismissal of the rumours? That’s up to interpretation. The claims that Microsoft is changing the pre-owned games model at retail are false or users will not have to pay a fee to play pre-owned games on Xbox One or there will be no change to how retailers sell pre-owned Xbox games in the future would have been a denial.

That the reports are inaccurate and incomplete is as frustratingly vague as every comment on the subject from Microsoft has been so far. The report could be inaccurate for an assortment of minor reasons, none of which affect its central claims.

And more to the point, if the claims are inaccurate then why not tell us when we shared them with you prior to publication?

Again we’re left in the situation of craving nothing more than a concrete response to what is fundamentally a very simple question: Under what circumstances will users be charged for playing a game that has previously been registered on another user’s account?

It sounds like we want the same thing, Major some clarification. We eagerly await.

Microsoft s Xbox One Controller Will Last Longer Than The Console Itself

The controller for Microsoft s upcoming Xbox One console can be mashed and smashed by gamers for the next decade. Microsoft accessories and hardware manager Bob Brown revealed in an interview with Pocket-Lint that there have been numerous rigorous tests the company put the Xbox One s controller through during its development. Microsoft tested 20 controllers over the past six months, pressing their buttons repeatedly between 4 to 5 times per second for a total of 2 million taps apiece. The thumbsticks are also worked over and over again to ensure reliability and the company even conducts a series of drop tests to ensure the controllers remain intact. The executive noted that controllers should last between seven and 10 years, or in some cases even longer. Given that Microsoft usually updates its console every five to eight years, the Xbox One s controller should still be alive and well when the company s next-generation system is released.

Developers Address Video Game Violence in New Film

Violence in video games is always a hot topic, but until now, the debate has been largely one-sided. As part of the upcoming film Video Games: The Movie, leading industry figures discuss the issue of violence in video games and what effect it has on the children and adults consuming them.

In a brutal teardown of the mainstream media mindset toward the topic, Mikey Neumann, creative designer at Gearbox Software, Cliff Bleszinski, creator of Gears of War, and a handful of other important industry figures tore into some of the common misconceptions and misdirected blame that occurs during these discussions.

Neumann dug deep, calling attention to the fact that blame is often

diverted from parents themselves and onto video games, It’s weird how when you watch the people and they go to Congress and they’re angry: ’Our kids are being corrupted.’ I’m like ’Yeah, exactly. Your kids. , he continued, They’re your children. You should be not corrupting them. ’I leave them alone ten hours a day, he’s getting corrupted by this.’ Well no s***. It’s like finding your dad’s Playboys under the bed and then blaming Playboy."

That’s not how legitimate scientific research works.

Brian Fargo, founder of InXile Productions, used the industry s strict rating system as an example of how games are meant to defend against underage players, We re just like any other industry that we have these rating systems in place and there s going to be something for everybody. This echo s Neumann s point that the parent is responsible for the content that their child can acquire, not the industry.

Bleszinski spoke to the illegitimacy of the connection between video games and violence, saying that, People like to make just kind of a causal link and say well video games cause violence. It’s like, let’s see, so, there’s more crime in the summer and more ice cream is sold in the summer, therefore ice cream causes crime. That’s not how legitimate scientific research works.

With the discussion on violence in video games popping up every time a tragedy occurs, it s reassuring to know that key members of the industry are ready to stand up and fight against misconceptions. Video Games: The Movie is expected to release in September 2013, and will continue to work against these misconceptions aimed at the video game industry.

Can Video Games Make Dyslexic Children Read Better?
Or how Rayman Raving Rabbids can make you read faster.

While the contention that video games are bad for kids is slowly, stubbornly slipping from the public conscious, it seems that study at the other end of the spectrum how video games might be good for children is still very much in its infancy, and often met with scepticism and disdain.

A recent example of this is a paper published in Current Biology earlier this year from The University of Padua, bearing the eye-catching title Action Video Games Make Dyslexic Children Read Better. The title is largely self-explanatory: the study claimed to show that young children aged 7-13 with dyslexia, a mental condition that can greatly hinder reading ability, could read faster after 80 minute play sessions of select minigames from Rayman Raving Rabbids. In some cases the results were equivalent to or even exceeded the effects of a whole year of traditional therapy. Such bold conclusions quickly drew headlines which, unsurprisingly, were followed by criticism from some in the field of neuroscience. I decided to investigate further.

Welcome to the Academy.

At first glance it sounds like a crazy idea, admits Simone Gori ,who wrote the paper along with Padua colleagues Andrea Facoetti and Sandro Franceshini. But previous studies showed that action video games improved attention, and we believed that this could translate directly

into better reading abilities. The outcome was a pleasant one.

Simone does his best to walk me through the complexity of his findings. Our study is the first to show how action video game experiences could potentially be useful in remediating a developmental disorder [like dyslexia]. Our research proved that training attention, without any reading or language training, directly translates into better reading abilities.

Dyslexia is arguably the most prevalent neuro-developmental disorder, affecting a large percentage of the population worldwide. Despite this, there remains fierce debate in the scientific community about its exact nature. The dominant view, despite lack of scientific evidence, is that dyslexia is exclusively a language problem, insists Simone. In fact, attentional deficits are proved to be a core deficit of dyslexia, while a causal link between language problems and dyslexia has yet to be found.

So, if dyslexia does stem from an attention deficiency rather than a language problem, video games, with their unrivalled (and oft-criticised) ability to sustain a child s attention, could prove hugely beneficial in treatment of the condition. It s with this in mind that the use of Rayman Raving Rabbids in a major scientific study begins to seem less ridiculous.

Simone ensures me that the game was ideal for his purposes, allowing the division of minigames into action and non-action categories. The distinction was based on criteria such as speed of transient events and moving objects, unpredictability, and peripheral processing. This allowed the study to closely differentiate which elements of the game elicited positive results. Only when subjects played the games that satisfied the action criteria was there improvement in their reading ability.

Perhaps it was inevitable that such bold conclusions would attract criticism. Most prominent is Dorothy Bishop, Professor of Developmental Neuropsychology at the Department of Experimental Psychology in Oxford, who declined to be interviewed for this article. On her high profile personal blog she criticised the extent of the testing, calling it methodologically weak due to the small sample groups. She refers to the seemingly significant results as false positives that wouldn t hold up to further testing. She concludes, If playing active computer games really does massively enhance children s reading, we might have expected to see a dramatic improvement in reading levels in the general population in the years since such games became widely available.

Criticisms [about the small test groups] are absolutely appropriate, but at the same time applied to most research at early stages, responds Dr. Paula Tallal, Co-director of The Centre of Molecular and Behavioural Neuroscience at Rutgers University. The vast majority of studies that have ever been done were special populations done with small groups of subjects. This is what science generally does: very small, controlled group studies to work out if it s even worthwhile to test any further.

The video games are increasing fluency and speed of processing. They re a scaffold upon which you can build fluency with what you already know.

Simone Gori agrees, and believes that personal motivations are to blame for his study being singled out for criticism. The reality is that people tend to use supposed methodological problems only when they don t like the results. He goes on to cite a long list of papers produced in the last 30

years of dyslexia study that also used a sample size of around 10 subjects.

What appears to have been lost in the criticism is how the study defines better in the context of reading ability. When it comes to reading there is a huge difference between fluency, the speed at which someone reads, and accuracy, which is the literal comprehension of language. The article didn t claim that they improved accuracy one bit, says Dr Tallal. It just improved the number of words per minute these kids could read. Action video games are not teaching children to read. These children already know what they know. The video games are increasing fluency and speed of processing. They re a scaffold upon which you can build fluency with what you already know.

There has also been concern voiced, both by Dorothy Bishop and John Rack, head of assessment services at the charity Dyslexia Action, that misunderstanding the study s definition of better could lead to some parents abandoning traditional dyslexia treatment and replacing it with sessions in front of the Xbox. Simone Gori believes such fears are unfounded. If you read all the media that we released after our study was published, caution was the key word. We never suggested quitting training to play video games instead. We wanted to open up future possibilities for dyslexia remediation.

The idea of replacing conventional therapy with video games sounds, on the surface, deeply irresponsible. Yet it isn t unprecedented. Penelope Trunk is a mother in the US who decided to take her sons out of school so that they could educate themselves. This involves copious amounts of gaming. Her youngest son, aged seven, has dyslexia, and she claims that video games have been hugely beneficial in overcoming his reading difficulties.

We had a private tutor for my son. It was not nearly as effective as video games, Penelope tells me. The biggest problem with dyslexia is that it makes reading so difficult that practicing isn t any fun. Video games are short bits of reading, sometimes just one or two word commands. And it s fun. It incentivises him to work harder. He d only read when the tutor told him to read. With a video game he can practice reading all day.

Although anecdotal, this certainly supports Simone Gori s theory of attentional deficit issues as a key component of dyslexia. A video game may not have the same level of educational content as a book, but its appeal to young people is likely to hold their attention for far longer, subsequently improving their ability to concentrate on other tasks such as reading. Dr Tallal elaborates on the broader potential of video games in dyslexia treatment.

A video game may not have the same level of educational content as a book, but its appeal to young people is likely to hold their attention for far longer

I was the first to develop the idea that you can use video game technologies to build specific neuroprocessing exercises that capitalise on the brain s remarkable ability to change with experience which is called neuroplasticity. We ve been able to work out what variables drive neuroplasticity most efficiently. They have to do with intensely focusing on information that individually adapts to your own abilities, that gets harder and harder, requires sustained attention, and offers timely rewards and immediate feedback. Video games are the perfect vehicle.

So while the Italian study was limited in some respects, this shouldn t

diminish the impact of its findings. Simone and his colleagues plan to test further, focusing on pre-reading age children to determine if age appropriate games at this stage in life can reduce future dyslexia incidence.

Uncertainty remains over whether other commercial action games would show the same benefits. Simone contends that All games that have the action characteristics [found in Rayman Raving Rabbids] should provide the same beneficial results. Dr Tallal is less certain. I don t know that you can generalise. I think you would have to try other games. Action video games is a general term; not all of them are going to have the same secret sauce, as it were, of rapid processing.

It seems, then, that the only consensus opinion, one way or another, is that further study is required to truly gauge the impact that video games could have on dyslexia treatment. Certainly it s too early for children to be abandoning traditional therapy in favour of lengthy Minecraft sessions. Yet it would also be a shame if the criticisms levelled at the study, which, as Dr Tallal is keen to stress, generally originate from personal blogs and not peer reviewed journals, were to hinder incredibly promising findings. If links between attentional deficits and dyslexia can be further established, it could position video games as a key element of treatment alongside other techniques, and help put an end to the lingering stigma attached to young people and their gaming habits.

 If action video games help kids get better, then that s an advance, concludes Dr Tallal. There s more science to do, no doubt. But if the games work, let the children play them.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
  """""""""""""""""""""

’Atari Dump’ Will Be Excavated, After Nearly 30 Years

The famed "Atari Dump" is about to excavated, as after nearly 30 years the New Mexico landfill where the game console maker buried its mistakes the biggest being the game E.T. The Extra-Terrestrial will be dug up by game developer Fuel Industries, which hopes to make a documentary about the project.

Also known as the Atari Graveyard or the E.T. Dump, the desert landfill is the spot where Atari decided to permanently off-load tons of games that were sitting unsold in a warehouse in El Paso, Texas, in 1983. So they went to a dump in Alamogordo, N.M., where this week to allow Fuel to excavate.

"That September, according to newspaper accounts, 14 trucks backed up to the dump and dropped their loads," the blog reports. "Company spokespeople told the local press that the waste was mostly broken and returned merchandise consoles, boxes, and cartidges."

The move came as Atari shifted its manufacturing business overseas to China. It also just had to find something to do with all those E.T. games.

"The rumor is that Atari decided to deal with its oversupply by simply burying all of those extra cartridges in the Alamogordo landfill, crushing them with bulldozers and covering them with cement," wrote in a caption for a photo of the dump taken in 2010.

"Reportedly, other items were also dumped, including returned Pac-Man cartridges, broken Atari computers, and perhaps even prototypes of unreleased hardware," Schrantz writes, engendering hopes (in a few people, anyway) that early versions of Atari's ill-fated might be among the finds.

As Western Digs reports, news of the excavation shows how the detritus of our electronic culture can morph into artifacts.

That's not to say that all outdated technology is mere trash: Consider that last weekend, a vintage Apple-1 computer, made in 1976, sold at auction for $671,400, as.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Pentagon Programs Target of China Cyber Threat

New revelations that China used cyberattacks to access data from nearly 40 Pentagon weapons programs and almost 30 other defense technologies have increased pressure on U.S. leaders to take more strident action against Beijing to stem the persistent breaches.

The disclosure, which was included in a Defense Science Board report released earlier this year, but is only now being discussed publicly, comes as Defense Secretary Chuck Hagel heads to Southeast Asia, where he will discuss the escalating cyberthreat with counterparts from a number of area nations.

While officials have been warning for years about China's cyber espionage efforts aimed at U.S. military and high-tech programs, the breadth of the list underscored how routine the attacks have become. And, as the U.S. looks to grow its military presence in the Asia Pacific, it heightens worries that China can use the information to blunt America's military superiority and keep pace with emerging technologies.

"It introduces uncertainty on how well the weapons may work, and it means we may have to redo weapons systems," said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies. "If they know how it works precisely, they will be able to evade it and figure out how to better beat our systems."

A chart included in the science board's report laid out what it called a

partial list of 37 breached programs, which included the Terminal High Altitude Area Defense weapon a land-based missile defense system that was recently deployed to Guam to help counter the North Korean threat. Other programs include the F-35 Joint Strike Fighter, the F-22 Raptor fighter jet, and the hybrid MV-22 Osprey, which can take off and land like a helicopter and fly like an airplane.

The report also listed another 29 broader defense technologies that have been compromised, including drone video systems and high-tech avionics. The information was gathered more than two years ago, so some of the data is dated and a few of the breaches such as the F-35 had actually already become public.

The details of the breaches were first reported by The Washington Post.

According to a defense official, the report is based on more than 50 briefings that members of the board's task force received from senior leaders in the Pentagon, the State Department, the intelligence community, national laboratories and business. The official was not authorized to discuss the report publicly so spoke on condition of anonymity.

U.S. officials have been far more open about discussing the China cyberattacks over the past year or two, beginning with a November 2011 report by U.S. intelligence agencies that accused China of systematically stealing American high-tech data for its own national economic gain. The Pentagon, meanwhile, in its latest report on China's military power, asserted publicly for the first time that Beijing's military was likely behind computer-based attacks targeting federal agencies.

"In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military," said the report, which was released earlier this month.

In Beijing on Wednesday, Assistant Foreign Minister Zheng Zeguang did not directly address the allegations, but said that China opposes all hacking and referred to an agreement with the U.S. to form a cybercrime working group.

Cybersecurity experts have for some time been urging the U.S. government to use sanctions or other punishments against China for the breaches.

The benefits to the cyber espionage are high and the costs are low, said Shawn Henry, former cyber director at the FBI and now president of CrowdStrike Services, a security technology company.

"There is no cost, there are no sanctions, no diplomatic actions, no financial disincentives," said Henry, adding that the U.S. intellectual property losses are in the hundreds of millions of dollars. He said that the U.S. needs to have a discussion with Chinese leaders about "what the red lines are and what the repercussions will be for crossing those red lines."

U.S. leaders, including President Barack Obama, however, have instead been using the bully pulpit to increase pressure on the Chinese to confront the problem. Obama is expected to raise the issue with China's new leader Xi Jinping during a summit next month in Southern California.

Pentagon Press Secretary George Little said Tuesday that the Pentagon maintains "full confidence in our weapons platforms," adding that the department has taken a number of steps to strengthen its network defenses and monitor for threats.

Defense contractors, meanwhile, declined to say whether their systems had been breached. But recent filings to shareholders indicate these companies see intrusions as a serious risk to their business, particularly when they must rely on third-party suppliers.

In its most recent annual report, Lockheed Martin a primary contractor on missile defense programs told shareholders that prior cyberattacks "have not had a material impact on our financial results," and that it believed its security efforts were adequate.

However, suppliers and subcontractors have "varying levels of cybersecurity expertise and safeguards and their relationships with government contractors, such as Lockheed Martin may increase the likelihood that they are targeted by the same cyber threats we face," according to the 2012 report.

In a statement emailed to reporters on Tuesday, Lockheed Martin said it has made "significant investments" in cybersecurity and that the company was trying to secure its supply chain given that "program information resides in a large cyber ecosystem."

Similar risk disclosures to shareholders have been made recently by Northrop Grumman, Boeing and Raytheon. For example, Northrop Grumman wrote in its 2012 annual report that cyber intrusions "could damage our reputation and lead to financial losses from remedial actions, loss of business or potential liability."

Company spokesman Randy Belote on Tuesday declined to say whether Northrop Grumman’s systems had been breached, citing company policy. But, he added, "the number of attempts to breach our networks (is) increasing at an alarming rate."

China Doesn’t Care if Its ’Digitalized’ Military Cyberwar Drill Scares You

In the face of fears from President Obama to the Pentagon and across the globe about the increasing military might behind Chinese hacking, China’s state news agency announced Wednesday that the nation’s People’s Liberation Army "will conduct an exercise next month to test new types of combat forces including units using digital technology amid efforts to adjust to informationalized war." You know, right after Obama and Chinese President Xi Jinping are meeting about the state of, among other things, a cyberwar going on underneath their noses.

The new report from Xinhua news agency adds that the drill, taking place on a large military training field and not some underground hack-a-thon bunker, "will be the first time a PLA exercise has focused on combat forces including digitalized units, special operations forces, army aviation and electronic counter forces." The terms "digitalized unit" and "electronic counter forces" don’t make it at all clear what China’s military has planned, but then again, no country is ever going to reveal its full cyberwarfare capabilities in detail and it’s not like it’s the first time the Chinese have tested the military reaches of their

digital warfare capabilities. Indeed, the U.S. was game to play along on more than one occasion. Last year it was reported that the U.S. and China had secretly engaged in at least two cyber war games in 2011, "designed to help prevent a sudden military escalation between the two superpowers if either felt they were being targeted," as ZDNet's Emil Potralinski reported. "In the first, both sides had to describe what they would do if they were attacked by a sophisticated computer virus, such as Stuxnet. In the second, they had to describe their reaction if the attack was known to have been launched from the other side." The first went better than the second, apparently, but neither appears to have taken place on a training base in Mongolia, as this new test will be when it's conducted by two army corps and eight military academies in "late June." Obama and Xi are set to meet at an estate in California on June 7-8. Cybersecurity is on the list of talking points, the White House confirmed Tuesday as National Security Advisor Tom Donilon visited Beijing ahead of the summit. Defense Secretary's Chuck Hagel is visiting Southeast Asia this week, and it's on his agenda, too.

News of China's "digitalized" drill comes on the heels of Tuesday's big Washington Post scoop that Chinese hackers had stolen designs for nearly 40 of the U.S.'s most valuable weapons programs and 30 defense technologies a move that could "weaken the U.S. military advantage in a future conflict." That article followed a Pentagon report earlier this month claiming that the Chinese government was directly connected to attacks on U.S. computer systems, which followed the cybersecurity firm Mandiant's report in February alleging that the PLA was connected to a number of cyberattacks on U.S. companies and infrastructure, and a 2012 assertion from national security veteran Richard Clarke that China has hacked every major U.S. company. Now, it appears, the secret training is out in the open.

Ireland Rejects U.S. Senator Claims as Tax Spat Rumbles On

Ireland has rejected claims by two U.S. senators that Ireland is a tax haven and had handed Apple Inc a special tax deal, a charge the pair stood by on Friday.

Ireland's ambassador to the United States Michael Collins has written to the two senators, Carl Levin and John McCain, arguing Ireland's tax system is transparent, according to the text released by the finance ministry.

But Levin and former U.S. presidential candidate McCain said records obtained by their committee showed Apple paid a nominal rate far below Ireland's statutory rate of 12.5 percent.

"Testimony by key Apple executives, including CEO Tim Cook and Head of Tax Operations Phillip Bullock, corroborates that Apple had a special arrangement with the Irish government that, since 2003, resulted in an effective tax rate of 2 percent or less," the senators said in a statement.

"Most reasonable people would agree that negotiating special tax arrangements that allow companies to pay little or no income tax meets a common-sense definition of a tax haven."

Ireland has been forced to defend its low corporate tax rate after the

Senate heard last week that the iPhone and iPad maker paid little or no tax on tens of billions of dollars in profits channeled through Irish subsidiaries and had effectively negotiated a special rate of less than 2 percent.

"Ireland’s tax system is set out in statute, so there is no possibility of an individual special tax rate being negotiated for companies," Collins wrote in the letter dated May 29 which was also sent to other members of Levin’s Senate subcommittee.

"The memorandum to the Permanent Subcommittee refers to Ireland as a ’tax haven’. As you will be aware, the OECD has identified four key indicators of a tax haven. None of these criteria applies to Ireland."

Dublin has begun a diplomatic offensive to repair the damage done to its reputation from the allegations. Finance Minister Michael Noonan said last week Ireland would not be the "whipping boy" for the U.S. Senate.

Ireland has said that if Apple paid tax at such low rates, it was down to tax planning where it had found a gap to exploit between two different tax jurisdictions. Dublin has called for international efforts to curb such large scale tax avoidance.

Apple’s Cook told a conference this week that the company did not have a special deal with the Irish government giving it a 2 percent flat tax rate.

Yet the Senate’s investigation showed the iPhone maker had paid tax worth just 2 percent of $74 billion in overseas income, largely helped by Irish tax law, which allows companies to be incorporated in the country without declaring taxes there.

The Senate subcommittee identified three Irish-registered Apple subsidiaries that have no tax residency in Ireland. One of these, a holding company that includes Apple’s retail stores throughout Europe, paid no tax at all in the last five years.

Cyber Threats Pose ’Stealthy, Insidious’ Danger

Defense Secretary Chuck Hagel said on Friday that cyber threats posed a "quiet, stealthy, insidious" danger to the United States and other nations, and called for "rules of the road" to guide behavior and avoid conflict on global computer networks.

Hagel said he would address cyber security in his speech on Saturday to the Shangri-La Security Dialogue in Singapore and the issue was likely to come up in a brief meeting with Chinese delegates on the margins of the conference.

"Cyber threats are real, they’re terribly dangerous," Hagel told reporters on his plane en route to the gathering. "They’re probably as insidious and real a threat (as there is) to the United States, as well as China, by the way, and every nation."

Cyber conflict could lead to "quiet, stealthy, insidious, dangerous outcomes," from taking down power grids to destroying financial systems or neutralizing defense networks, Hagel said.

"That’s not a unique threat to the United States, (it affects) everybody, so we’ve got to find ways here ... working with the Chinese, working with everybody, (to develop) rules of the road, some international understandings, some responsibility that governments have to take," he said.

Hagel’s remarks came two days after news reports said the Defense Science Board - a committee of civilian experts who advise the Defense Department - had concluded that Chinese hackers have gained access to the designs of more than two dozen major U.S. weapons systems in recent years. The Pentagon downplayed the report as outdated and overstated.

But the Defense Department underscored its concern about Chinese hacking in a separate report to Congress earlier this month, accusing Beijing of using cyber espionage to modernize its military.

The report said the U.S. government had been the target of hacking that appeared to be "attributable directly to the Chinese government and military."

Asked about Hagel’s comments, Chinese Foreign Ministry spokesman Hong Lei said China wanted to exchange views with U.S. officials on "relevant issues" on the sidelines of the Singapore meeting.

"We believe that on this issue both sides should sit down and carry out an even-tempered discussion," Hong told a daily briefing, referring to cyber security.

"We should make the cyber security issue a highlight of bilateral cooperation and make joint efforts to maintain an open, cooperative, secure and transparent cyberspace," he said.

President Barack Obama has made cyber security a priority of the administration and will discuss his concerns with Chinese President Xi Jinping in a meeting in California next week, White House spokesman Jay Carney said this week.

Hagel told reporters on his plane to Singapore that he had invited Chinese Defense Minister Chang Wanquan to visit the United States and a trip was being organized for August.

Asked whether it was effective to deal with the issue by publicly naming China, Hagel said he thought both public diplomacy and private engagement were necessary. Public statements are necessary to let people know what is going on, he said, but it doesn’t solve problems.

"The United States knows ... where many of these incursions come from," Hagel said. "It’s pretty hard to prove that they are directed by any specific entity, but we can tell where they come from. And I think we’ve got to be honest about that."

The problem will ultimately be solved by more private discussions, he added. "But it has to be public as well and we’ll deal with this. We must deal with this. This is a very dangerous threat to all of us."

Hagel is due to spend two days at the Shangri-La dialogue, engaging in bilateral and trilateral meetings with his Asian counterparts. He helped gain support for the annual dialogue as a U.S. senator more than a decade ago and was a leader of the first U.S. congressional delegation to the

event.

After Singapore, Hagel will travel to a NATO ministerial meeting in Brussels that will hold its first review of cyber defense, a sign the issue is climbing to the top of the alliance’s agenda due to concerns its infrastructure and secrets are vulnerable.

NATO Secretary-General Anders Fogh Rasmussen has said NATO systems face "regular" computer attacks. Of particular concern are the systems used to coordinate military actions among the 28 allied nations.

Hagel said cyber security would be a centerpiece of the NATO defense ministers meeting, adding "we all need to find ways, international standards, agreements" to commit to responsible use of cyber and "deal with these real threats."

Google Said To Face New Antitrust Probe Over Display Ads

Google Inc. is facing a new antitrust probe by the U.S. Federal Trade Commission into whether the company is using its leadership in the online display-advertising market to illegally curb competition, people familiar with the matter said.

The fresh inquiry, which follows the FTC s decision to close a review of Google s search business in January without taking action, is in the preliminary stages and may not expand into a larger probe, said the people, who asked not to be named because the matter hasn t been made public.

FTC investigators are examining whether Google is using its position in U.S. display ads - a $17.7 billion industry that includes the sale of banner ads on websites - to push companies to use more of its other services, a practice that can be illegal under antitrust laws, the people said. Google has been drawing regulatory scrutiny around the world as it bolsters its market share of digital advertising.

Canada s Competition Bureau is preparing to start a formal inquiry into Google s search practices, the company disclosed last week. The European Union is investigating Google for the way it operates the search business and also has opened a probe into its handset unit, Motorola Mobility, over the licensing of its patents to rival device makers. Antitrust agencies in Argentina and South Korea are also scrutinizing the company.

Niki Fenwick, a spokeswoman for Google, and Peter Kaplan, a spokesman for the FTC declined to comment on the probe.

Google, avoiding a potentially costly legal battle with U.S. regulators, ended a 20-month probe in January of whether it unfairly skewed search results by pledging to change some business practices and settling allegations it misused patents to thwart competitors in smartphone technology.

The company said it would voluntarily remove restrictions on the use of its online search-advertising platform and offer companies the option of keeping their content out of Google s search results.

The FTC s resolution of its search-practices probe came as a blow to

Google s competitors including Microsoft Corp., Yelp Inc. and Expedia Inc. An alliance of such e-commerce and Web-search companies pressed the agency to bring a lawsuit, claiming Google s dominance of Internet search, combined with the company favoring its own services in answers to queries, violates antitrust laws.

Microsoft isn t involved in the FTC s review of the display advertising market, one of the people said.

The FTC secured clearance to move forward with the new investigation in the display-advertising market from the antitrust division of the Justice Department under a process that ensures the two agencies don t investigate the same matters at the same time, one of the people said.

For the past two years, the antitrust division and the FTC have split investigations of the Mountain View, California-based company, with the FTC conducting a broad probe of whether Google s business practices hurt competition and the antitrust division reviewing its acquisitions.

In the new probe, the FTC is exploring concerns about Google s growing market share with some of its digital advertising tools and services, including technology that places display ads on websites, the people said.

The FTC is looking at whether Google is using its tools to force companies to bypass competing products and use other Google properties, including a marketplace for buying and selling Internet display ads, and features that help companies maximize revenue, the people said. The agency is also reviewing Google s potential to use its dominance in search advertising to squeeze out competitors in the display advertising market, the people said.

Some of the advertising tools came from Google s purchase of DoubleClick Inc., which received antitrust approval at the end of 2007. The FTC, which voted 4-1 to approve the merger, said competition among display-ad networks was dynamic, according to a statement at the time.

 We will closely watch these markets and, should Google engage in unlawful tying or other anticompetitive conduct, the commission intends to act quickly, the FTC said in the statement.

Google s share of the display ad market reached 24 percent during the first quarter in the U.S. with its closest competitors, Yahoo! Inc. and Facebook Inc., each holding less than 10 percent market share, according to research firm IDC.

Facebook, the largest social-networking service, lost its lead to Google last year and is expected to expand its market share at a slower pace. Facebook will grab 16 percent in 2015, up from 15 percent last year and less than 3 percent in 2008, EMarketer, another research firm, estimates.

Google took 47 percent of total U.S. digital ad spending in the first quarter of this year, according to IDC.

 The market positions of Google and DoubleClick suggest that the combined firm could engage in a number of potential anticompetitive strategies to further enhance its positions in the various markets at issue, the FTC wrote in its DoubleClick statement.

The practice of tying, or bundling, products and services together may be

a violation of antitrust laws if the company in question has the market power to force customers to acquire products or services together that they might prefer to buy from different providers, said Spencer Waller, an antitrust law professor at Loyola University Chicago.

One of the most high-profile tying cases was the lawsuit the U.S. brought against Microsoft in 1998, when it claimed the company unlawfully protected its Windows monopoly by keeping computer makers from promoting Web browsers that competed with Microsoft s Internet Explorer.

The government contended Microsoft hindered access to the Netscape Navigator browser because its Java programming language let programmers write applications that ran on any operating system, not just Windows. The final judgment, a settlement in which Microsoft agreed to end the anticompetitive conduct, put the company under court supervision until 2011.

Specialty producers may be very good at what they do, but if they can t get access to their customers, that s a legitimate harm that antitrust has addressed historically and should continue to address, Waller said.

Facebook Says Needs To Improve Response to Hate Speech

Facebook Inc admitted its systems to remove hate speech haven’t worked as well as the company had hoped, amid reports that advertisers were pulling their brands off the social network in the face of a backlash from women’s groups.

In a blog post by its safety team late Tuesday, the company acknowledged there had been problems with removing content that would be considered examples of gender-based hate.

"We have been working over the past several months to improve our systems to respond to reports of violations, but the guidelines used by these systems have failed to capture all the content that violates our standards. We need to do better - and we will," the company said in the post.

The British edition of MediaWeek reported on Wednesday that at least 13 brands pulled ads from Facebook in the wake of the campaign. The New York Times cited Japanese automaker Nissan as saying it had pulled all advertising off the social network until it received assurances that its ads would not appear alongside offensive content.

On Wednesday, Nissan spokesman David Reuter clarified that the company had asked Facebook to remove its ads from offensive pages that were visited by targeted users, and only from the British version of the social network. He said the automaker was not changing its advertising strategy with Facebook, with which it maintained a good relationship.

In its blog post on Tuesday, Facebook said it would update the guidelines used to evaluate hate speech, and would encourage existing online anti-hate groups to add representatives of women’s organizations as well.

Last week, a group called Women, Action & the Media released an open letter to Facebook, urging the company to improve its response to content that "trivializes or glorifies violence against girls or women."

They also called for Facebook members to contact advertisers whose ads appeared next to such content.

Facebook Cracks Down on Hate Speech Against Women

If Facebook were a city, these would be its seedy back alleys user-generated groups filled with jokes about rape and domestic violence, captioned over gruesome images of assaulted women.

But after protesters sent some 60,000 tweets to advertisers making note such posts, Facebook this week announced that it is stepping up efforts to eliminate such gender-based hate speech from the site, apologizing that it had failed to capture all the content that violates our standards.

The announcement came on the heels of a week-long social media campaign by women's rights activists, organized around the hashtag #FBRape, which brought down a barrage of thousands of angry tweets and letters on Facebook and, especially, its advertisers.

Facebook is locked in near-constant fights over its content, ranging from users rallying against changes to the site s layout to those demanding increased privacy settings and more protection of their data.

But what helped lift the #FBRape campaign above the fray of the standard social networking chatter, experts say, may have been the demographic that launched it: women.

Women are the muscle of the social media world, making up the majority of users on sites like Facebook, spending more time and creating more content than their male counterparts, according to Lee Rainie, director of the Pew Research Center s Internet Project.

Want your top political issues explained? Get customized DC Decoder updates.

We re not a marginalized group on these sites, says Soraya Chemaly, a writer and activist who was among the leading organizers of the campaign. This isn t some pet project special interest they re supporting it s more than half their users.

So far anyway, Facebook seems to have gotten the message. In a blog post Tuesday evening, the company announced that it would update its guidelines around hate speech, ensure its employees were accurately identifying prohibited content on the site, and take steps to prevent users from posting such content anonymously.

When people have to use their real names, it enforces social norms, says Gerald Kane, an associate professor of information systems at Boston College and an expert on social media. You re not going to misbehave as much if your friends are watching you.

Organized by activist groups Women, Action, and the Media (WAM) and the Everyday Sexism Project, along with Ms. Chemaly, the #FBRape campaign began last week with a call for Facebook users to contact companies whose ads were appearing on pages beside the violent and misogynist content and

call for them to withdraw their advertising from the site.

At issue were not just the violent images themselves, but also the fact that Facebook was failing to delete them when users flagged the photos as hate speech. In one screenshot posted to the WAM site, a user had reported an image of a woman shot in the head with the caption, I like her for her brains. Below it, an automated response from the site read, We reviewed the photo you reported, but found it doesn t violate Facebook s Community Standard.

Over the next week, activists sent out more than 5,000 e-mails and more than 60,000 tweets to advertisers, according to WAM, prompting more than a dozen companies including Nissan to pull ads from Facebook.

Facebook, meanwhile, responded almost immediately to the campaign, says Jaclyn Friedman, executive director of WAM. She says the protest's organizers were in touch with the company by Thursday of last week, and had begun discussing how the company could improve its policies.

Facebook, after all, has a reason to be responsive in this case, Ms. Friedman says. We re the reason these sites exist, the people on whose data these companies make money. And women increasingly aren t accepting their treatment in these spaces.

A study released in April by the Pew Internet Project found that, of all Internet users, 71 percent of women used social networking sites, compared with just 62 percent of men. Female social media users in North America spend an average of 12 hours on social media each week, according to a separate study by the global communications firm Weber Shandwick.

So there s good reason to take their interests under account, Mr. Kane says. At the same time, Facebook doesn t want to police the boundaries of good taste, and anyway, a site with a user base of 1 billion can do only so much to ward off bad apples.

They don t want to be purveyors of hate, he says, but a certain segment of the population will probably always be ugly.

Maine Teens Wary of Social Media After Homicide

The death of a 15-year-old Maine girl allegedly killed in a bizarre kidnapping plot involving a fake Facebook profile has prompted some of her classmates to scale back their social media use or ditch it altogether.

Nichole Cable was allegedly killed by an acquaintance who used a fake profile to lure her from her home, then kidnap her in hopes of becoming a hero when he miraculously "found" her, according to state police.

Meanwhile, rumor and speculation ran rampant on social media following Cable's disappearance and the charging of a 20-year-old who knew her.

Ashley Pattershall said Thursday some of her classmates at Old Town High School have opted to deactivate their Facebook accounts.

"A couple of my friends have deleted their Facebook, and some of my friends don't have Facebook anymore," said the 16-year-old Pattershall, who was a close friend of Cable.

Kyle Dube, 20, of Orono, used a phony Facebook account created in the name of a student from another school to lure Cable outside her Glenburn home, where he abducted and killed her on May 12, authorities said. Her body was found more than a week later in a wooded area of Old Town, north of Bangor.

Dube told others he wore a disguise to kidnap Cable and intended to return later and find her safe and sound, police said. Instead, he discovered she was dead when he went to check on his duct-taped victim in the back of his father’s pickup.

Authorities said Dube told his girlfriend and brother that he dumped Cable’s body and covered it with sticks. He was formally charged Wednesday with murder and kidnapping.

Dube’s attorney, Stephen Smith, did not immediately return a phone call left at his Bangor office on Thursday.

Cable’s mother, Kristin Wiley, said Thursday that she wants to brainstorm with school principals about how to help teens be safe online. A police officer also talked to her about doing seminars on teen safety, she said.

"We need to get awareness out. Even the Bible says, ’Do not stand idle by.’ I’m not going to stand idle. For my daughter, I will not stand idle. I will do whatever I can," she said from her Glenburn home.

According to state police, detectives interviewed a young man named Bryan Butterfield a day after Cable was reported missing. Butterfield told police that someone had created a phony Facebook account in his name, and police traced it to Dube’s parents’ house in Orono.

Cable was frequently contacted by the fake Butterfield and agreed to meet with him at the end of her road to get some marijuana the night she went missing, according to the state police affidavit.

Social media’s role in Nichole’s disappearance and death was a wakeup call for students, many of whom have become paranoid about online contacts, said Pattershall, Cable’s friend.

Pattershall, who said the fake Butterfield account had contacted her and others, said she cleaned out her Facebook "friend" lists, making sure only confirmed friends and family members can communicate with her.

Wiley choked up as she talked about how her neighbors looked out for each other on the dirt road with a handful of houses in Glenburn.

She still has difficulty fathoming the state police account of Dube jumping out to grab her daughter at the end of the road.

"It’s very important that we prevent this from happening again, not just in our community but any community, Wiley said.

Wiley said her daughter would want her to act.

"She would not want anyone else to go through this."

USSR’s Old Domain Name Attracts Cybercriminals

The Soviet Union disappeared from the map more than two decades ago. But online an ’e-vil empire’ is thriving.

Security experts say the .su Internet suffix assigned to the USSR in 1990 has turned into a haven for hackers who’ve flocked to the defunct superpower’s domain space to send spam and steal money.

Capitalist concerns, rather than Communist nostalgia, explain the move.

"I don’t think that this is really a political thing," Oren David, a manager at security firm RSA’s anti-fraud unit, said in a recent telephone interview. David noted that other obscure areas of the Internet, such as the .tk domain associated with the South Pacific territory of Tokelau, have been used by opportunistic hackers.

"It’s all about business," he said.

David and others say scammers began to move to .su after the administrators of Russia’s .ru space toughened their rules back in late 2011.

Group-IB, which runs one of Russia’s two official Internet watchdogs, says that the number of malicious websites hosted across the Soviet Union’s old domain doubled in 2011 and doubled again in 2012, surpassing even the vast number of renegade sites on .ru and its newer Cyrillic-language counterpart.

The Soviet domain has "lots of problems," Group-IB’s Andrei Komarov said in a phone interview. "In my opinion more than half of cybercriminals in Russia and former USSR use it."

The most notorious site was Exposed.su, which purportedly published credit records belonging to President Barack Obama’s wife, Michelle, Republican presidential challengers Mitt Romney and Donald Trump, and celebrities including Britney Spears, Jay Z, Beyonce and Tiger Woods. The site is now defunct.

Other Soviet sites are used to control botnets the name given to the networks of hijacked computers used by criminals to empty bank accounts, crank out spam, or launch attacks against rival websites.

Internet hosting companies generally eliminate such sites as soon as they’re identified. But Swiss security researcher Roman Huessy, whose abuse.ch blog tracks botnet control sites, said hackers based in Soviet cyberspace can operate with impunity for months at a time.

Asked for examples, he rattled off a series of sites actively involved in ransacking bank accounts or holding hard drives hostage in return for ransom brazenly working in the online equivalent of broad daylight.

"I can continue posting this list for ages," he said via Skype.

The history of .su goes back to the early days of the Internet, when its architects were creating the universe of country code suffixes meant to mark out a website’s nationality. Each code like .fr for France or .ca for Canada was meant to correspond to a country.

Some Cold War-era domain names such as .yu for Yugoslavia or .dd for

East Germany evaporated after the countries behind them disappeared. But the .su domain survived the dissolution of the Soviet Union in 1991 and the creation of a .ru domain in 1994, resisting repeated attempts to wipe it from the Web because, unlike other defunct domains, those behind .su refused to pull the plug on both commercial and patriotic grounds.

With more than 120,000 domains currently registered, mothballing .su now would be a messy operation.

"It’s like blocking .com or .org," said Komarov. "Lots of legitimate domains are registered there."

Among them are stalin.su, which eulogizes the Soviet dictator and the English-language chronicle.su, an absurdist parody site.

But experts say many are fraudulent, and even the organization behind .su accepts it has a problem on its hands.

"We realize it’s a threat for our image," said Sergei Ovcharenko, whose Moscow-based nonprofit Foundation for Internet Development took responsibility for .su in 2007.

Ovcharenko insisted that only a small number of .su sites are malicious, although he acknowledged that criminal sites can stay online for extremely long periods of time. He said his hands were tied by weak Russian legislation and outdated terms of service. But he promised that stricter rules are on their way after months of legal leg work.

"We are almost there," he said. "This summer, we’ll be rolling out our new policy."

Meanwhile .su has become an increasingly notorious corner of the Internet, an online echo of the evil empire moniker assigned to the Soviet Union by U.S. President Ronald Reagan 30 years ago.

David, the RSA manager, said the emergence of a Communist relic as a 21st century security threat was a bizarre blast from the past.

"I thought that the Berlin Wall and my grandma’s borscht are the only remnants of the Soviet Union," he said. "I was wrong."

Linked In Jumps on the 2-Step Password Train Because It Looks Good

A little less than a year after six million passwords got hacked from the site, LinkedIn has added the more secure two-step verification, probably to look just as responsible as all the other tech sites adding a step these days. LinkedIn hasn’t had a breach since the high-profile hack last June, but after Google, Facebook, and most recently Twitter fending off phishing the second step involves texting a passcode to your cellphone, although Twitter makes you enter it with every login the social network for business people needed to look more professional than ever and has added the functionality, the company announced in a blog post Friday.

Some might call it overkill to so thoroughly protect a site that doesn’t really have that much personal information. (Though, LinkedIn members do provide credit card details to pay for premium subscriptions.) But it’s good to get in the habit of doing a lot more leg-work to make sure, you

know, someone doesn’t sabotage your rsumØ. The future is in doubly sure password protection. Plus, as far as hackers are concerned, one site is just the gateway to another before you know it, they’re inside your email and running rampant.

Sick of Typing Passwords? Get an Electronic Tattoo or Ingest a Pill

The average person inputs a password 39 times a day, with power users typing that string of letters and numbers up to 100 times a day, Motorola’s head of Advanced Technology & Projects Regina Dugan revealed at the All Things D conference this week.

But even then that password, as a series of recent hacks have shown, isn’t always secure.

Sure, there are ways of authenticating beyond passwords, including two-factor authentication which requires a user to input a password and a code that is sent to their phone, but Motorola’s dreaming up a way of keeping our passwords even closer to ourselves - literally.

At the conference Dugan showed off two ways of turning your body into a password. With an electronic tattoo, she said, people would be able to just wear their password on their skin.

"We are thinking of a variety of options for how you could do better at authentication. You can start with near term things like tokens or fobs, but you can also think of a means of authentication that you could wear on your skin for a week at a time," she said. "We are talking about an electronic tattoo."

Motorola is working with a company called MC10, which makes a tattoo with embedded sensors and an antenna. "What we plan to do is work with them to advance a tattoo for authentication. Ten- to 20-year-olds might not want to wear a watch on their wrists, but you can bet they will wear a tattoo - if only to piss off their parents," she said.

MC10 has shown off this technology before but in a medical sense. The tattoos could replace pacemakers, MC10’s CEO said at TedMed back in 2012.

But Dugan is thinking beyond the outside of our bodies with authentication: "I take a vitamin every morning. What if I could take vitamin authentication?"

Dugan showed off a small pill. Inside that pill wasn’t medication but a tiny computer chip. "It also has what amounts to an inside-out potato battery. The acids in your stomach serve as an electrolyte and power it up," she explained.

That creates a signal in your body and your body becomes the password. You can touch your phone, car or door and be "authenticated in." Sounds crazy, yes, but this is not just "science fiction" Dugan said. Made by Proteus Digital Health, the pill was approved by the FDA in August 2012. Its version of the digital pill sends information to your doctor from inside your body. It is currently being tested with placebo pills.

So when is all of this coming? Not as soon as Motorola’s made-in-America Moto X phone. Motorola’s CEO Dennis Woodside said, "This isn’t stuff that

is going to ship anytime soon, but having the boldness to think differently about problems everyone has everyday is really important for Motorola now."

Microsoft Windows 8.1 Features Detailed: Start Button Revival and App Improvements Coming

The Start button is getting a fresh start.

Microsoft has revealed some of the changes coming to Windows 8.1 and, as expected, it has resurrected the Start button in the left-hand corner of the operating system to make it easier for users who choose to use a mouse and keyboard.

The button was removed in Windows 8, the touchscreen-centric software that was released on laptops, desktops and tablets in October.

But that’s just one of many new additions Microsoft plans to add to Windows 8.1, which will be out later this year as a free upgrade for Windows 8 users.

The operating system is still centered around the Start Screen, which is full of tiles or apps. In Windows 8.1, however, there are new tile sizes and it is easier to move around the blocks. You press and hold the tiles now, similar to how you can rearrange apps in Android.

There are other small changes, too. For instance, when you download a new app, it won’t automatically be added to your Start Screen now, it will be put in a new app view.

Microsoft has also improved its own apps. The new global search function will now search Bing and the Music and Photos apps have been redesigned. It’s also easier to use two apps at once now. You can still put two apps side by side with Snap, but you can change the sizes of the windows and now you can run three apps side by side.

The biggest app improvement though might be Internet Explorer 11. The new browser has speed and touchscreen improvements. Additionally, instead of having to swipe down from the top of the screen to make the address bar or tabs appear, you can set them to be always-visble. Those tabs will also sync across Windows 8.1 computers and tablets.

While Microsoft has heard the call for some simpler navigation around the operating system, it also added some fun features. In Windows 8.1, you will be able to add a slideshow of photos to the lock screen. There are also more colors and backgrounds for the Start Screen, including animated graphics.

Microsoft CFO and CMO of Windows Tami Reller told ABC News last month that one of the major pieces of feedback about Windows 8 had to do with non-touchscreen computers.

"We’ve focused on a number of improvements to ensure easier navigation for people using a mouse and keyboard," Antoine Leblond, corporate vice president of Windows Program Management, said in a blog post. "We’ve improved the way you navigate to Start with the mouse by changing the Start ’tip’ to be the familiar Windows logo."

Clicking on the Start tip in the lower left-hand corner will bring you back to the Start Screen. No, you won't get the traditional Start menu. Microsoft will announce other Windows 8.1 features in the next few months, Leblond said in the post. The company has acknowledged that while 100 million Windows 8 licenses have been sold since the release in late October, users have complained about the big changes.

"We've learned a lot from customers in how they are using the product and have received a lot of feedback," Leblond said. "We've been watching, we've been listening.

"Windows 8.1 will continue to build on what you love bringing the latest advancements in hardware, apps, cloud services and the OS to enable a unique experience in everything you do."

NH Senate Postpones Action on Social Media Bill

People interested in whether New Hampshire will join about a dozen other states in prohibiting bosses from requiring employees or job applicants to disclose a user name or password to personal social media or email accounts will have to wait another week.

The Senate put off a vote planned on the bill Thursday. The bill would not prohibit an employer from obtaining information about an employee or job applicant that is in the public domain, or prevent the employer from investigating whether the employee is complying with securities or financial laws based on the person's personal website used for business purposes.

The ban would only apply to the worker's personal accounts unrelated to the employer's business, and would not prevent employers from enforcing workplace policies about company equipment.

New Gmail Inbox Will Auto-Organize Incoming Mail

Google is about to make some big changes to its popular Gmail that will make it easier to sort email. Today the search giant announced a new style and some additional features, which are set to roll out soon.

Android, iOS, and desktop users will be treated to a new inbox feature that offers automatic organization of incoming mail into groups.

The "Primary" category will contain messages from friends and family, as well as any other messages that don't appear in other tabs. Another tab called "Social" will automatically contain notifications and messages from social networks sites, like your Facebook notifications or Twitter follower alerts. The "Promotions" group will capture deals, offers and promotions from places like shopping or coupon websites.

Bills, receipts, and confirmation emails will be organized into the "Updates" group, and messages from online groups, discussion boards and mailing lists will appear in the "Forums" group.

The inbox organization groups are optional, and a user can choose which of the five categories, if any, they want to use.

But Google isn't the first to have automatic sorting features. Microsoft and other e-mail add-ons have offered similar features. Microsoft's Outlook.com has a feature called Sweep, which sweeps messages based on their categories into their own folders. Other e-mail apps like Sanebox and Unroll.me have similar sorting features.

Google, however, is bringing its features not just to the web. Users of the Gmail Android or iOS apps will see their Primary inbox tab upon opening the app, but Google has made accessing the other inbox groups easier with swipe gestures and large labels.

The new inbox features will roll out over the next few weeks, but if you can't wait, Google says be on the lookout for it in the Gmail settings menu. You will be able to enable it yourself.

Wearable Technology Emerging as Major Technology Cycle

Wearable computing is emerging as the type of significant technology shift that will drive innovation in the way personal computing did in the 1980s or mobile computing and tablets are doing currently, said Kleiner Perkins Caufield & Byers partner Mary Meeker at the All Things D conference on Wednesday.

While technology cycles generally last 10 years, she said wearables were coming on stronger and faster than is typical. The change is noteworthy because major technology cycles often support tenfold growth in users and devices, she said in her annual report on the state of the Internet.

Many of the 150 times or so per day that users interact with their phones - to look for messages, make calls, check the time, and the like - could be hands-free with wearable technology, she said.

"Some people laugh at wearables..." read one slide featuring an image from the TV show "Saturday Night Live" that mocked Google glass, a wearable technology. As the audience chuckled, she brought up the next slide, reading "Some people laughed at PC & Internet." The slide showed a 1999 Barron's cover trumpeting the headline "Amazon.Bomb."

Later in the morning, Twitter chief executive Dick Costolo picked up the theme, telling conference goers that it was clear wearable technology would play a large role in the future, even if what is perhaps the most-discussed example - Google glass - doesn't emerge as the first mainstream hit.

Speaking last night at the conference, Apple CEO Tim Cook stopped short of clarifying if Apple was working on wearable products amid speculation that it is developing a smart watch, saying only that wearable computers had to be compelling.

He added that Google's Glass is likely to have only limited appeal.

Meeker also reviewed themes she has highlighted in the past, including the remarkable growth of mobile technology and the Chinese economy, and the ceding of power from traditional personal computing companies to phone and

tablet makers.

7 Tips For Checking Facebook at Work

You may be a social media junkie, hopping from one site to another. But if your employer suspects you check your friend’s Facebook wall more than your work emails, he may be entitled to make you hand over your passwords.

Lawmakers across the country have begun weighing social media privacy laws that bar employers from hiring or firing employees for not surrendering an account username or password. Social media privacy laws have been introduced or are pending in 35 states, according to the National Conference of State Legislators, an organization that tracks legislation at the state level. Since the beginning of this year, five states - including Arkansas, Colorado, New Mexico, Utah and Washington - have enacted legislation that prohibits employers from accessing social media passwords of employees.

But even as attempts to shield employees from intrusive employers grow, some laws feature exceptions that allow companies to snoop. The recently passed Utah law permits employers to request passwords for social media accounts such as Facebook or Twitter when a device is supplied or paid for in whole or in part by the company. An employer can also gain access to company-sponsored accounts managed by employees.

If your state has yet to address the issue, you could fall under an employer policy that grants wide authority in acquiring social media information. About 24 percent of businesses monitor social media information, according to a 2012 survey of 1,105 employees by the Chicago-based talent management software company SilkRoad. A 2011 survey by the Society of Corporate Compliance and Ethics revealed that 42 percent of companies punish employees for behavior on social media websites, up from 24 percent in 2009. The survey received responses from 485 public and private companies as well as nonprofits.

If you’re worried your tweets or Facebook posts may jeopardize your job, follow these steps:

1. Learn your company’s policies. If your state lacks a social media privacy law, your employer may have one. The policy may not ban usage all together, but it may lay out explicit guidelines. Learn what you can and can’t do, says Tyson Snow, an employment attorney at Pia Anderson Dorius Reynard & Moss, LLC in Salt Lake City. "With that knowledge you can tailor your actions accordingly," he says.

2. Learn the state law. If you work in a state that does have a social media privacy law, or is on the cusp of passing one, read up on it. You don’t necessarily have to read the bland text of the law, but newspaper articles, magazines or online blogs, can help you understand what your state allows under the law, Snow says.

3. Go private on your profile. An inquisitive boss may be inclined to look up what you’ve been doing on Facebook or Twitter during office hours. Without privacy settings, he or she won’t have to go through a potential legal fuss to wrangle your username and password. Snow recommends setting your privacy settings "to ensure that someone who is not your friend or follower or isn’t a general member of the public

doesn’t have access to your content."

4. Pay attention to company culture. Working for a tech savvy company like Google or Microsoft, you may have free license to browse your social media pages during a shift, says Terri Thompson, an etiquette coach in Kentucky. If a policy is unclear, examining the actions of colleagues is one way to determine when visiting Facebook or Twitter is permissible. But Thompson says to lay the burden for spelling out the policy on the employer. "It needs to be communicated, maybe even as early as the interview process," she says.

5. Be mindful when using company gear. It’s a great deal: Your company provides and picks up the tab for your laptop and iPhone. But if personal exchanges between co-workers or friends and family are edgy, if not outright inappropriate, then isolate your use to a personal device. "If you’re an employee, and you don’t want your employer to have access to any of your information, then don’t access social media sites off your employer-provided computer or employer-provided cellphone," Snow says.

6. Self-monitor your time. The company you work for may have a lax policy, leaving you to either keep your roaming habits in check or letting them run amok. Thompson recommends brief exchanges and limiting usage to breaks and your lunch hour. "What can’t and doesn’t need to happen is being constantly on it," she says.

7. Gracefully guide the company account(s). Wanting to make a splash across several social media platforms, your company may want you to take the reins of its newly created accounts. Thompson recommends not revealing internal deliberations and straying away from posting anything text or images that can be construed as negative. "Be very, very careful that you’re only ... putting the company in the most positive light possible," she says.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.